

**Menetelmä ja järjestelmä palvelun tarjoamiseksi tietoverkon välityksellä –
Förfarande och anordning för att bjuda service i ett datanät**

Keksinnön kohteena on menetelmä ja laitteisto palvelun tarjoamiseksi tietoverkkoa käyttäen. Erityisesti keksintö koskee palvelutapahtumaan liittyvien tunnistetietojen välittämistä eri osapuolten ja -järjestelmien välillä.

Tietoverkoissa, kuten Internetissä ja matkapuhelinverkoissa uusien tuotteiden ja palvelujen tarjonta ja kysyntä on lisääntynyt voimakkaasti. Eräänä palveluna mainittakoon esimerkiksi erilaiset maksulliset viestit tai sanomat sekä palvelut ja tuotteet, joita on saatavilla useisiin erityyppisiin päätelaitteisiin käyttäjätarpeen mukaan, joita päätelaitteita voivat olla esimerkiksi PC (Personal Computer), PDA (Personal Digital Assistant), matkapuhelin ja digiTV (digitaalinen televisio). Lisäksi avoimissa verkoissa on nykyisin tarjolla entistä useammin erinäisiä verkkolomakkeita tai asiakirjoja tai sen kaltaisia palveluja, joiden käyttämiseen vaaditaan käyttäjän tunnistaminen ja todentaminen tai käyttöoikeus.

Internetissä ja vastaavissa avoimissa verkoissa tapahtuviin rekisteröitymisiin, osapuolten tunnistamiseen ja todentamiseen sekä viestien, erilaisten asiakirjojen ja dokumenttien lähettämiseen, välittämiseen ja vastaanottoon liittyvään tietoturvallisuuden parantamiseen tunnetaan erilaisia keinoja, kuten esimerkiksi käyttäjätunnuksen ja salasanan käyttö. Salasanat voivat olla kiinteitä tai vaihtuvia. Salasanat ovat usein kuitenkin hankalia muistaa niiden paljouden tai monimutkaisuuden takia, sillä lähes jokaiseen palveluun, jossa yksilön tunnistaminen tai todentaminen on välttämätöntä, on käyttäjällä oltava oma käyttäjätunnus ja salasana. Aina ei suinkaan ole mahdollista, että käyttäjän tunnus ja salasana olisivat joka järjestelmässä samoja eikä se tietoturvallisuuden kannalta ole edes järkevää. Lisäksi tunnukset ja salasanat generoidaan usein mielivaltaisesti käytettävän järjestelmän taholta ja salasanat täytyy yleensä vaihtaa tietyin väliajoin, jolloin salasanojen muistaminen on entistä vaikeampaa.

Ennestään tunnetaan ratkaisuja salausta vaativien palvelujen hoitamiseksi mm. US-julkaisuista 5 220 510 ja 5 870 724. Mainittujen julkaisujen mukaisissa ratkaisuissa käytetään käyttäjäkohtaisia salasanat tai käyttäjän yksilöiviä tunnuslukuja järjestelmissä, jotka muodostavat yhteyden suoraan esimerkiksi pankin ja päätelaitteen välille tyypillisesti ATM-verkon välityksellä. Julkaisusta WO 0031608 tunnetaan myös ratkaisu, jossa kannettavan päätelaitteen tunnuslukua voidaan käyttää tunnis-

tettaessa käyttäjä hänen kytkeytyessään esimerkiksi tietokoneeseen tai järjestelmään. Lisäksi myös EP-julkaisusta 0 960 402 tunnetaan ratkaisu langattoman päätelaitteen, kuten matkapuhelimen, käytöstä pankki- ja laskunmaksupalveluissa siten, että päätelaitteessa on erillinen ns. matkapuhelinlompakko-moodi.

- 5 Tunnettujen ratkaisujen mukaisiin järjestelyihin liittyy kuitenkin eräitä epäkohtia. Ratkaisut ovat tyypillisesti tarkoitettu pelkästään tietyn pankin tai pankkipalvelun hoitamiseen. Ratkaisujen mukaisissa järjestelmissä on yleensä oma erillinen näppäimistö ja näyttö erityisesti pankkipalveluiden hoitamiseen eikä järjestelmien mukaisia laitteita yleensä voi käyttää laajemmin. Esimerkiksi tietoverkoissa käsiteltäviä
- 10 lomakkeita ei yleisesti voi sähköisesti allekirjoittaa puuttuvan toimikortin ja lukijan vuoksi. Tunnetuissa menetelmissä ongelmana on lisäksi teleoperaattoreiden, palveluntuottajien ja muiden toimijoiden palveluja ja verkkoteknologioita yhdistävän tunnistamis-, todentamis- ja maksamisen menetelmän puute. Verkkopalveluissa tarvitaan tehokkaita ja luotettavia maksamisen, tunnistamisen ja todentamisen menetelmiä ja rakenteita sekä järkeviä tuote-, palvelu- ja hinnoituskonsepteja. Tunnettujen
- 15 ratkaisujen toimintamallit ja palvelukäytännöt eivät mahdollista järkevien ja laaja-alaisen sähköisten palvelujen kehittämistä kuluttajien, yritysten ja viranomaisten tarpeisiin.

- 20 Keksinnön tavoitteena on luoda ratkaisu palvelun tarjoamiseksi siten, että edellä mainittuja tekniikan tasoon liittyviä epäkohtia voidaan vähentää. Keksintö pyrkii ratkaisemaan sen, kuinka ostotapahtumaan tai palveluun liittyvä tieto saadaan varmennettua eri osapuolten taholta ja kuinka palvelunkäyttäjät tai osapuolet voidaan tunnistaa ja todentaa yksiselitteisesti.

- 25 Keksinnön tavoitteet saavutetaan siten, että palvelunkäyttäjän päätelaitteelle lähetetään varmennuspyyntö, jonka palvelunkäyttäjä voi hyväksyä syöttämällä päätelaitteeseensa tunnuksen. Tunnus voi olla esimerkiksi nelinumeroinen tunnusluku tai vaihtoehtoisesti siinä voi olla myös kirjaimia tai erikoismerkkejä.

- 30 Keksinnön mukaiselle menetelmälle palvelun tarjoamiseksi tietoverkossa on tunnusomaista se, että siirretään avoimessa verkossa palvelutapahtumaan liittyvää tietoa, hyväksytään mainittu tieto ja suoritetaan tiedon hyväksyjän tunnistaminen suljetussa verkossa suoritettavan todentamisen avulla.

Keksinnön mukaiselle järjestelmälle palvelun tarjoamiseksi tietoverkossa on tunnusomaista se, että järjestelmä käsittää avoimen ja suljetun tietoverkon, välineet palvelutapahtumaan liittyvän tiedon siirtämiseksi avoimessa verkossa, välineet maini-

tun tiedon hyväksymiseksi ja välineet tiedon hyväksyjän tunnistamiseksi suljetussa verkossa suoritettavan todentamisen avulla.

Keksinnön eräitä edullisia suoritusmuotoja on esitetty epäitsenäisissä patenttivaatimuksissa.

- 5 Keksinnön avulla saavutetaan huomattavia etuja tekniikan tason ratkaisuihin verrattuna. Keksinnön mukainen menetelmä mahdollistaa palvelunkäyttäjän tunnistamisen ja vahvan todentamisen esimerkiksi käyttäjän päätelaitteen, kuten matkapuhelimen, avulla. Keksinnön avulla voidaan mm. avoimessa tietoverkossa tarjottavaan palveluun tai tapahtumaan liittyviä tietoja tai varmistuspyyntöjä lähettää luotettavasti suljetussa verkossa olevaan palvelunkäyttäjän päätelaitteeseen varmistusta, käyttäjän identifioimista tai tietojen hyväksymistä varten.

Lisäksi keksinnön avulla on mahdollista suorittaa luotettavasti tapahtumaan liittyvien molempien osapuolten tunnistaminen, siirrettävien asiakirjojen tai dokumenttien oikeaksi todistaminen ja alkuperän varmistaminen, tietojen luottamuksellisuuden ja eheyden varmistaminen, tapahtuman tai toimenpiteen kiistämättömyys sekä tapahtuma-ajankohdan rekisteröinti.

- 15 Keksinnön avulla voidaan hoitaa myös notaaripalveluja, kuten aikaleimoja ja arkistointia. Notaaripalveluja vaaditaan mm. sähköisten viestien ja sanomien, virallisten tai virallisuonteisten asiakirjojen ja dokumenttien toimittamisessa, jakelussa ja säilyttämisessä. Näitä toimintoja varten tarvitaan tietoverkkomaailmassa ns. kolmas luotettava osapuoli (KLO), joka on riippumaton kaikista muista palveluketjuun kuuluvista osapuolista tai sähköisten lomakkeiden lähettäjistä ja vastaanottajista. KLO voi sijaita tietyssä kohtaa palveluketjua palvelutapahtumaan liittyvien osapuolten välissä, jossa se tarjoaa roolinsa mukaisia varmennuspalveluita, kuten osapuolten tunnistamista ja todentamista.

Tässä patenttihakemuksessa käytetään mm. seuraavia käsitteitä:

- "Asiakas" on keksinnön mukaisen menetelmän käyttäjä ja kauppatapahtuman osapuoli, joka hankkii tai ostaa tuotteen tai palvelun esimerkiksi perinteisesti myyjältä tai vaihtoehtoisesti tietoverkossa tai sen kautta.
- 30 - "Avoimen verkon palveluntuottaja" voi olla esimerkiksi Internet-operaattori, joka tuottaa tietoverkkopalveluita. Lisäksi avoimen verkon palveluntuottaja voi tarjota sähköisiä verkkolomakkeita esimerkiksi tietoverkkojen välityksellä

sekä toimia osapuolten tunnistajana ja osapuolten välisenä tietojen välittäjänä.

- 5 - ”Avoimen verkon päätelaite” voi olla esimerkiksi sopivilla muistiyksiköillä, tietoliikennetyöyhteydellä ja prosessorilla varustettu tietokone tai työasema, PDA, matkapuhelin, digiTV tai vastaava järjestelmä. Avoimen verkon päätelaite voi olla yhteydessä avoimen verkon palveluntuottajan järjestelmään joko suoraan avoimen verkon välityksellä tai vaihtoehtoisesti suljetun verkon välityksellä esimerkiksi jos päätelaite on kytketty langattomaan päätelaitteeseen, kuten matkapuhelimeen.
- 10 - ”Digitaalinen allekirjoitus” perustuu ns. julkisen avaimen menetelmään, jolla tunnistetaan ja todennetaan viestin lähettäjä ja vastaanottaja, taataan toimipiteen kiistämättömyys sekä varmistetaan tietojen luottamuksellisuus ja eheys.
- 15 - ”Kolmas luotettava osapuoli” yhdistää palvelun tuottajan ja käyttäjän tarjoamalla roolinsa mukaisia varmennuspalveluita, kuten osapuolten tunnistamisen ja todentaminen.
- ”Lähettäjä” lähettää viestin tai sanoman sähköisessä muodossa vastaanottajalle.
- 20 - ”Myyjä” on keksinnön mukaisen menetelmän käyttäjä, joka myy esimerkiksi tuotetta tai palvelua joko perinteisesti kauppapaikallaan tai vaihtoehtoisesti tietoverkossa tai sen kautta.
- ”Palvelunkäyttäjä” on esimerkiksi asiakas, myyjä, yksityinen kuluttaja tai kansalainen, yritys tai yhteisö, viranomainen tai julkishallinto, joka käyttää keksinnön mukaista menetelmää tai mainittuja palveluntuottajan palveluja.
- 25 - ”Sanoma, pyyntö tai viesti” voi käsittää sähköisessä muodossa esimerkiksi yleisen tunnisteen tai tunnisteosan, vastaanottajan nimen tai verkko- tai hakemisto-osoitteen, verkkopalvelun tuottajan nimen ja osoitteen sekä sähköpostiosoitteen. Lisäksi se voi olla esimerkiksi kokonainen asiakirja tai dokumentti, sähköpostiviesti liitetiedostoineen, itsenäinen julkaisu, tuote tai palvelu, tiedote tai tiedonanto, huomautus tai muistutus, hälytys tai virheilmoitus, palvelu- tai tarjouspyyntö, kehote tai opaste, ilmoitus tai mainos, lupa tai haaste. Kaikille näille on yhteistä se, että ne on toimitettu, julkaistu tai välitetty vastaanottajalle sähköisessä muodossa.
- 30

- "Suljetun verkon palveluntuottaja" voi olla esimerkiksi matkapuhelinoperaattori, joka välittää viestejä ja sanomia tai tietoja esimerkiksi Internet- ja langattomissa verkoissa ja voi toimia osapuolten tunnistajana ja osapuolten välisenä tietojen välittäjänä.
- 5 - "Suljetun verkon päätelaite" voi olla esimerkiksi PDA, matkapuhelin tai vastaavan kaltainen laite. Erityisesti päätelaite voi olla langattomassa verkossa toimiva matkapuhelin, joka on varustettu sopivalla SIM-kortilla (Subscriber Identity Module).
- 10 - "Sähköinen lomake" on jollakin sähköisellä välineellä tuotettu, välitetty tai jaettu, näytetty tai täytetty määrämuotoinen lomake, joka usein on kopio alkuperäisestä paperilomakkeesta.
- "Todentaminen" varmistaa järjestelmän käyttäjän tunnistamisen oikeellisuuden.
- 15 - "Tunnistaminen" on tapahtuma, jossa käyttäjä kertoo järjestelmälle identiteettinsä eli tunnistetiedot. Tunnistetiedot voidaan vaihtoehtoisesti lukea myös käyttäjän lähettämästä viestistä tai sanomasta.
- "Varmennus tai varmenne" sisältää osapuolten tai palvelun tunnistetiedot, viittauksen käyttöoikeuksiin, viestien tai sanomien salausavaimet ja digitaalisen allekirjoituksen vaatimat salaiset avaimet ja varmenteen myöntäneen tahon eli liikkeellelaskijan tiedot.
- 20 - "Vastaaottaja" ottaa hänelle sähköisesti lähetetyn viestin tai sanoman vastaan.
- "Verkkolomakkeella" tarkoitetaan kehitettyä älykästä sähköistä lomaketta, jossa määrämuotoisuuden lisäksi on toiminnallisia ominaisuuksia, kuten esitäyttö, opasteet ja liittyä sovellukseen tai suoraan tietokantaan, eikä sillä yleensä ole yhteen vastinetta tai suhdetta paperilomakkeeseen. Verkkolomaketta on myös mahdollista verrata perinteiseen sovelluksen näyttöön. Yhtenä älykkään lomakkeen kriteerinä voidaan myös pitää tietojen haku- tai täyttömahdollisuutta sekä digitaalista allekirjoitusta.
- 25
- 30 Tarkastellaan ensimmäisenä esimerkkinä avoimessa verkossa tapahtuvaan palvelu- tai kauppatapahtumaan liittyvien tapahtumatietojen välittämistä osapuolten välillä. Osapuolia eli palvelukäyttäjiä tässä tapauksessa ovat myyjä ja asiakas. Esimerkissä

myyjäosapuoli tarjoaa kauppapaikallaan tuotteitaan tai palveluaan. Asiakas kerää ostoksensa ostoskoriin, josta myyjä siirtää kauppapahtuman tiedot omaan kassa- ja laskutusjärjestelmään. Maksutapahtumassa kauppapahtuman tiedot lähetetään myyjän laskutusjärjestelmästä tietoverkon, kuten Internetin välityksellä palveluntuottajan tai operaattorin järjestelmään ja sieltä edelleen langattoman suljetun verkon välityksellä asiakkaan päätelaitteelle.

Asiakas tunnistetaan ja todennetaan palveluntuottajan avulla, minkä jälkeen voidaan aloittaa kauppapahtumatietojen käsittely asiakkaan päätelaitteella niin, että asiakas voi varmistua saapuneiden tietojen, kuten loppusumman ja ajankohdan, oikeellisuudesta ja että ne liittyvät juuri hänen kauppapahtumaansa.

Jos asiakas hyväksyy hänen päätelaitteelle lähetetyt palveluun tai kauppapahtumaan liittyvät tiedot, kuten esimerkiksi laskun, voidaan maksaminen suorittaa antamalla päätelaitteelle tunnus, joka voi olla esimerkiksi matkapuhelimen tapauksessa matkapuhelimen PIN-luku (Personal Identification Number). Vastaavasti myyjä saa tiedon asiakkaan maksusuorituksesta tietoverkkojen välityksellä kassa- tai laskutusjärjestelmäänsä.

Seuraavaksi tarkastellaan esimerkkinä tietoverkoissa, kuten Internetissä tarjottavaa sähköistä asiointipalvelua. Tässä esimerkissä palvelunkäyttäjä voi olla esimerkiksi yksityinen käyttäjä, jolla on käytössään avoimen verkon päätelaite, kuten tietokone tai työasema, ja suljetun verkon päätelaite, kuten matkapuhelin. Esimerkissä selaimella noudetaan sähköisiä lomakkeita palveluntuottajan palvelimelta palvelunkäyttäjän työasemalle toimenpiteitä, kuten tietojen hakua, täyttämistä tai allekirjoittamista varten. Viimeistelty lomake voidaan allekirjoittaa digitaalisesti työasemasta riippumattoman ja fyysisesti erillään olevan langattoman päätelaitteen avulla ja lähettää avoimessa verkossa vastaanottajalle.

Jos sähköinen lomake päätetään allekirjoittaa digitaalisesti ennen lähetystä, palvelunkäyttäjä lähettää allekirjoituspyynnön palveluntuottajalle. Allekirjoituspyyntö voidaan lähettää joko palvelunkäyttäjän työasemalta tai langattomalta päätelaitteelta. Tämän jälkeen palveluntuottaja tyypillisesti vahvistaa ja välittää allekirjoituspyynnön palvelunkäyttäjän langattomaan päätelaitteeseen tunnistettuaan ja todennettuaan avoimessa ja suljetussa verkossa olevat päätelaitteet. Allekirjoitus voidaan suorittaa digitaalisesti antamalla suljetussa verkossa olevalle palvelunkäyttäjän päätelaitteelle tunnus. Digitaalinen allekirjoitus toimitetaan palvelunkäyttäjien tunnistajana ja todentajana toimivan palveluntuottajan välityksellä palvelunkäyttäjän työasemalle,

jossa palvelunkäyttäjä voi liittää sen digitaalisesti allekirjoitettavaan lomakkeeseensa tai muuten suorittaa asianmukaiset toimenpiteet.

Edellä mainittu suljetussa verkossa toimiva asiakkaan tai palvelunkäyttäjän päätelaite on tyypillisesti PDA, matkapuhelin tai vastaavan kaltainen järjestelmä, jolla voidaan hyväksyä vastaanotettu pyyntö tai varmenne esimerkiksi näppäilemällä tietty tunnus. Erityisesti päätelaite voi olla langattomassa verkossa toimiva matkapuhelin, joka on varustettu sopivalla SIM-kortilla (Subscriber Identity Module). Päätelaitteessa voi lisäksi olla prosessori sekä tietty salausavain, joka voi olla sijoitettu esimerkiksi laitteen SIM-korttiin.

- 10 Edellä mainittu avoimessa verkossa toimiva palvelunkäyttäjän tai myyjän päätelaite voi olla esimerkiksi sopivilla muistiyksiköillä, tietoliikenneyhteydellä ja prosessorilla varustettu tietokone tai työasema, PDA, matkapuhelin, digiTV tai vastaava järjestelmä, jolla voidaan lähettää ja vastaanottaa edellä mainitun kaltainen pyyntö, varmenne tai palvelu.
- 15 Edellä mainituissa esimerkeissä tietoverkossa tapahtuvalle sähköiselle asioinnille asetetaan tiettyjä perusvaatimuksia, kuten osapuolten tunnistaminen ja todentaminen, tapahtuman ja toimenpiteen kiistämättömyys ja ajankohdan rekisteröitävyys, tietojen luottamuksellisuuden ja eheyden varmistaminen, asiakirjan oikeaksi todistaminen ja alkuperän varmistaminen sekä notaaripalvelut, kuten aikaleima ja arkistointi. Lisäksi voidaan vaatia välitettävän tiedon salaus käyttämällä määrättyjä salausalgoritmeja. Tiedon salaus ja salauksen purkaminen voidaan edullisesti suorittaa esimerkiksi suljetussa verkossa olevan palvelunkäyttäjän päätelaitteen, päätelaitteessa olevaan SIM-korttiin tallennetun salausavaimen ja päätelaitteessa mahdollisesti olevan prosessorin avulla.
- 20
- 25 Seuraavassa osiossa selostetaan keksinnön eräitä edullisia suoritusmuotoja hieman tarkemmin viitaten oheisiin kuviin, joissa

kuva 1 esittää vuokaaviona erästä suoritusmuotoa palveluun liittyvän varmuksen hyväksymiseksi keksinnön mukaisesti,

- kuva 2 esittää erästä keksinnön mukaista järjestelmää tuotteen tai palvelun maksamiseksi,
- 30

kuva 3 esittää erästä keksinnön mukaista järjestelmää lomakkeen digitaaliseksi allekirjoittamiseksi,

kuva 4 esittää vuokaaviona erästä menetelmää tuotteen tai palvelun maksamiseksi keksinnön mukaisesti, ja

kuva 5 esittää vuokaaviona erästä menetelmää lomakkeen digitaalisesti allekirjoittamiseksi keksinnön mukaisesti.

- 5 Kuva 1 esittää vuokaaviona erästä suoritusmuotoa keksinnön keskeisestä ideasta tarjottavaan palveluun liittyvän varmennuksen hyväksymiseksi. Tarjottava palvelu on tyypillisesti kauppatapahtuma tai ostosuoritus, mutta palvelu voi olla myös sähköisen lomakkeen digitaalinen allekirjoittaminen, palveluun rekisteröityminen tai muu vastaava palvelu, jossa vaaditaan palvelunkäyttäjän luotettavaa tunnistamista ja
- 10 todentamista. Keksinnön idean mukaisesti voidaan suorittaa luotettavasti myös tapahtumaan liittyvien molempien osapuolten tunnistaminen, siirrettävien asiakirjojen tai dokumenttien oikeaksi todistaminen ja alkuperän varmistaminen, tietojen luottamuksellisuuden ja eheyden varmistaminen, tapahtuman tai toimenpiteen kiistämättömyys, tapahtuma-ajankohdan rekisteröinti sekä aineiston arkistointi.

- 15 Tässä esimerkissä palvelunkäyttäjiä ovat myyjä, jolla on avoimessa verkossa oleva päätelaite ja asiakas, jolla on suljetussa verkossa oleva päätelaite. Myyjä voi lisäksi olla myös luonteeltaan palveluntarjoaja, joka tarjoaa palveluita avoimessa verkossa.

- Palvelua voidaan tarjota 101 ja käyttää esimerkiksi tyypillisessä kauppaympäristössä, jolloin avoimen verkon palvelunkäyttäjä eli myyjä voi siirtää tapahtumatiedot suljetun verkon palvelunkäyttäjän eli asiakkaan päätelaitteeseen eri tietoverkkojen välityksellä. Palvelu voi olla vaihtoehtoisesti myös tietoverkossa tarjottavaa palvelua, kuten esimerkiksi ns. verkkokauppaa, jolloin tapahtumatietojen välittäminen asiakkaan päätelaitteeseen voidaan suorittaa automaattisesti. Jos asiakas käyttää esimerkiksi palvelua, jossa vaaditaan käyttäjän tunnistamista tai palveluun liittyvien
- 25 tietojen varmistamista käyttäjän taholta, voidaan vaiheessa 102 lähettää asiakkaalle varmennuspyyntö esimerkiksi tämän suljetun verkon päätelaitteelle avoimen ja suljetun verkon sekä näiden verkkojen palveluntuottajien avulla. Varmennuspyyntö voi sisältää palvelutapahtumaan liittyvää tietoa tai sillä voidaan varmistua asiakkaan henkilöllisyydestä ja siten mahdollisesti myös tämän oikeuksista tarjottavaan palveluun. Vaiheessa 103 voidaan tunnistaa varmennuspyynnön lähettäjä ja/tai vastaanot-
- 30 taja esimerkiksi avoimen tai suljetun tai molempien verkkojen palveluntuottajien avulla.

Pyyntö voidaan lähettää esimerkiksi avoimessa verkossa olevalla myyjän päätelaitteella, kuten tietokoneella, jolloin pyyntö edullisesti lähetetään ensin avoimen ver-

kon palveluita toimittavalle palveluntuottajalle, joka voi tunnistaa ja todentaa pyynnön lähettäneen osapuolen. Avoimen verkon palveluntuottaja voi välittää pyynnön edullisesti suljetun verkon palveluntuottajalle, kuten esimerkiksi matkapuhelinoperaattorille, joka puolestaan voi tunnistaa ja todentaa pyynnönsaajan eli asiakkaan päätelaitteen. Suljetun verkon palveluntuottaja voi tämän jälkeen välittää pyynnön asiakkaan päätelaitteelle.

Saatuana varmennuspyynnön pyynnönsaaja eli asiakas voi tarkistaa pyynnössä olevat tiedot ja joko hyväksyä pyynnön tai kieltäytyä hyväksymästä sitä. Jos asiakas päättää hyväksyä pyynnön, voidaan hyväksyminen suorittaa vaiheessa 104 syöttämällä suljetun verkon päätelaitteeseen tunnus. Annettava tunnus on edullisesti päätelaitteen PIN-luku, mutta se voi olla myös jokin muu käyttäjäkohtainen tunnusluku. Tunnus todennetaan vaiheessa 105 esimerkiksi päätelaitteen SIM-kortin avulla. Vaiheessa 106 hyväksytty varmennus lähetetään myyjälle. Lähetetty varmennus välitetään edullisesti esimerkiksi suljetun tai avoimen verkon palveluntuottajan tai vaihtoehtoisesti molempien avulla, jotka voivat tunnistaa asiakkaan tai molemmat osapuolet vaiheessa 107 ja välittää varmennuksen edelleen myyjälle. Saatuana hyväksytty varmennuksen, myyjä voi antaa asiakkaalle esimerkiksi oikeuden palvelun tai tuotteen käyttöön. Asiakkaan päätelaitteellaan hyväksymä pyyntö tai varmenne voidaan välittää vastaavaa tietoliikennelinkkiä pitkin takaisin myyjälle, kuin mitä linkkiä pitkin pyyntö välitettiin myyjältä asiakkaan päätelaitteelle. Tällöin asiakkaan ja myyjän tunnistaminen ja todentaminen voidaan suorittaa luotettavasti esimerkiksi suljetun ja avoimen verkon palveluntuottajien avulla.

Välitettävän tiedon virallisuudesta tai tärkeydestä riippuen tieto voidaan toimittaa vaihtoehtoisesti myös tietoverkoissa notaaripalveluja tarjoavan kolmannen luotettavan osapuolen (KLO) välityksellä. KLO voi sijaita määrätysssä kohtaa palveluketjua palvelutapahtumaan liittyvien osapuolten välissä. Notaaripalveluja tai KLO:n toimintoja ei tämän hakemuksen yhteydessä kuvata tai määritellä tarkemmin.

Kuva 2 esittää keksinnön erään suoritusmuodon mukaista järjestelmää 200 maksusuoritukseen tai muuhun kauppatapahtumaan tai palveluun liittyvän tiedon hyväksymiseksi asiakkaan 223 päätelaitteella 207. Suoritusmuodon mukaisessa menetelmässä myyjä 224 siirtää kauppatapahtumaan liittyvän tiedon kassa- ja laskutusjärjestelmäänsä 201, josta tapahtumatiedot lähetetään avoimen verkon 202, kuten Internetin (I) välityksellä palveluntuottajan järjestelmään 203 vaiheessa 1.0. Avoin verkko voi vaihtoehtoisesti olla myös jokin muu tiedonsiirtämiseen tarkoitettu ratkaisu. Tapahtumatiedot voivat sisältää tietoa esimerkiksi tapahtuma-ajasta, myyjästä 224,

tuotteesta, ostajasta tai asiakkaasta 223 sekä tunnisteeseen, jolla asiakas 223 tunnisteetaan. Tunniste voi olla esimerkiksi viitteellinen asiakastunnus.

Avoimen verkon palveluntuottaja 203 voi tunnistaa myyjän 224 tai asiakkaan 223 saadessaan tapahtumatiedot myyjän järjestelmästä ja välittää 204 tiedot edelleen suljetun verkon palveluntuottajalle 205, joka lähettää tiedot edelleen asiakkaan 223 päätelaitteelle 207 suljetun verkon 206 välityksellä vaiheessa 1.1. Myös suljetun verkon palveluntuottaja 205 voi tässä vaiheessa tunnistaa myyjän 224 sekä asiakkaan 223 ja tämän langattoman päätelaitteen 207. Palveluntuottaja 205 on tyypillisesti esimerkiksi langattoman verkon verkko-operaattori, kuten matkapuhelinoperaattori, joka välittää viestejä ja sanomia tai tietoja langattomissa verkoissa. Palveluntuottaja 205 voi välittää tietoa myös Internetissä. Langaton verkko 206 voi olla esimerkiksi matkapuhelinverkko.

Kauppatapahtumatietojen käsittely voidaan suorittaa asiakkaan 223 päätelaitteella 207 tyypillisesti siten, että asiakas voi varmistua saapuneiden tietojen oikeellisuudesta, kuten loppusummasta, tapahtuma-ajasta ja siitä, että tiedot liittyvät hänen kauppatapahtumaansa. Kauppatapahtumatietojen hyväksyminen, kuten maksaminen, voidaan suorittaa asiakkaan 223 päätelaitteella 207 antamalla päätelaitteelle esimerkiksi edellä mainitun tyyppinen tunnus. Tunnuksen antamisen jälkeen kauppatapahtuman hyväksymiseen liittyvä tieto voidaan lähettää suljetun verkon palveluntuottajalle 205 suljetun verkon 206 välityksellä vaiheessa 2.0, joka palveluntuottaja välittää 204 tiedon edelleen avoimen verkon palveluntuottajalle 203. Myyjä 224 saa tiedon asiakkaan maksusuorituksesta omaan järjestelmäänsä 201 palveluntuottajalta 203 avoimen verkon 202 välityksellä vaiheessa 2.1.

Myös kauppatapahtuman hyväksymiseen liittyvän tiedon välitysvaiheessa sekä suljetun verkon palveluntuottaja 205 että avoimen verkon palveluntuottaja 203 voivat tunnistaa asiakkaan 223 tai tämän päätelaitteen 207 sekä myyjän 224 tai tämän järjestelmän 201. Lisäksi kauppatapahtumaan liittyvät tiedot voidaan välittää kolmannen luotettavan osapuolen välityksellä, joka voi luotettavasti tunnistaa tapahtuman osapuolet.

Myyjän 224 kassa- ja laskutusjärjestelmässä 201 on tyypillisesti välineet 208 palvelutapahtumaan liittyvän tiedon lähettämiseksi avoimen tai suljetun verkon palveluntuottajalle sekä välineet 219 palvelutapahtuman hyväksymiseen liittyvän tiedon vastaanottamiseksi. Avoimen verkon palveluntuottajan järjestelmässä 203 on yleensä välineet 209 palvelutapahtumaan liittyvän tiedon lähettäjän tunnistamiseksi sekä välineet 217 palvelutapahtuman hyväksymiseen liittyvän tiedon vastaanottajan tun-

nistamiseksi ja välineet 218 palvelutapahtuman hyväksymiseen liittyvän tiedon siirtämiseksi myyjän 224 järjestelmään 201.

Suljetun verkon palveluntarjoajan järjestelmässä 205 on tyypillisesti välineet 210 palvelutapahtumaan liittyvän tiedon vastaanottajan tunnistamiseksi, välineet 211 palvelutapahtumaan liittyvän tiedon siirtämiseksi asiakkaan päätelaitteelle 207 sekä välineet 216 palvelutapahtuman hyväksymiseen liittyvän tiedon lähettäjän tunnistamiseksi. Asiakkaan 223 päätelaitteessa 207 on yleensä välineet 212 palvelutapahtumaan liittyvän tiedon vastaanottamiseksi, välineet 213 palvelutapahtumaan liittyvän tiedon hyväksymiseksi, välineet 214 päätelaitteella 207 annetun tunnuksen tunnistamiseksi, välineet 215 palvelutapahtumaan liittyvän tiedon siirtämiseksi suljetun verkon palveluntuottajalle 205 tai avoimen verkon palveluntuottajalle 203, prosessori 222 sekä SIM-kortti 220, jossa SIM-kortissa on edullisesti tallennettuna salaussalvain 221 tiedon salaamiseksi ja salauksen purkamiseksi.

Lisäksi suljetun verkon palveluntuottajan 205 ja avoimen verkon palveluntuottajan 203 järjestelmissä on välineet tiedonsiirtämiseksi toistensa välillä esimerkiksi tiedonsiirtoon tarkoitetun järjestelmän 204 avulla. Lisäksi palveluntuottajien 203, 205 järjestelmissä voi olla keskenään samoja välineitä, jolloin tietojen välittäminen myyjän 224 päätelaitteen 201 ja asiakkaan 223 päätelaitteen 207 välillä voidaan hoitaa joko vaihtoehtoisesti vain suljetun verkon tai vain avoimen verkon palveluntuottajan välityksellä.

Kuva 3 esittää erästä keksinnön mukaista järjestelmää 300 avoimessa verkossa 202 tarjottavan sähköisen asiointipalvelun käyttämiseksi, jossa menetelmässä noudetaan sähköisiä verkkolomakkeita palveluntuottajan palvelimelta 203 palvelunkäyttäjän 223 päätelaitteelle 301, kuten työasemalle tai tietokoneelle, avoimen tietoverkon 202, kuten Internetin (I) välityksellä vaiheessa 1.0. Verkkolomakkeet voidaan noutaa päätelaitteelle 301 esimerkiksi toimenpiteitä, kuten tietojen hakua, täyttämistä tai digitaalista allekirjoittamista varten. Lomakkeiden nouto voi tapahtua esimerkiksi päätelaitteessa 301 olevan selaimen avulla tai lomakkeet voidaan vaihtoehtoisesti toimittaa myös muilla tavoin, kuten esimerkiksi levykkeellä, sähköpostitse tai muulla vastaavalla tiedonsiirtoon ja -välittämiseen tarkoitetulla menetelmällä. Lisäksi palvelunkäyttäjää 223 voi itse tuottaa käsiteltävänä olevan lomakkeen omalla päätelaitteellaan 301. Esimerkin mukainen palveluntuottaja 203 on tyypillisesti tietty yritys, yhteisö, viranomainen tai julkishallinto ja erityisesti palveluntuottaja voi olla Internet-operaattori, joka tuottaa tietoverkkopalveluja ja välittää tietoa esimerkiksi avoimessa verkossa olevan palvelunkäyttäjän 223 päätelaitteen 301, kuten työase-

man tai tietokoneen, ja suljetussa verkossa olevan palvelunkäyttäjän 223 päätelaitteen 207, kuten matkapuhelimen, välillä.

Palveluntuottaja 203 saa tyypillisesti kuittauksen lomakkeen vastaanotosta palvelunkäyttäjältä 223, joka käyttäjä voi esimerkiksi muokata, allekirjoittaa, lähettää tai arkistoida sähköisen lomakkeen tai asiakirjan. Jos palvelunkäyttäjä 223 haluaa allekirjoittaa sähköisen lomakkeen, voi hän lähettää päätelaitteellaan 301 allekirjoituspyynnön tai -sanoman palveluntuottajalle 203 avoimen tietoverkon 202 välityksellä vaiheessa 2.0. Allekirjoituspyyntö voidaan lähettää myös palvelunkäyttäjän 223 suljetun verkon päätelaitteelta 207. Avoimen verkon palveluntuottaja 203 voi tässä vaiheessa 2.0 tunnistaa palvelunkäyttäjän 223 päätelaitteen 301 (tai 207) ja välittää 204 allekirjoituspyynnön edelleen suljetun verkon palveluntuottajalle 205, joka voi jatkolähettää pyynnön esimerkiksi palvelunkäyttäjän langattomaan päätelaitteeseen 207 suljetun langattoman verkon 206 välityksellä vaiheessa 2.1. Myös suljetun verkon palveluntuottaja 205 voi tässä vaiheessa tunnistaa palvelunkäyttäjän ja tämän langattoman päätelaitteen 207.

Palvelunkäyttäjä 223 voi halutessaan allekirjoittaa päätelaitteella 207 vastaanottamansa sanoman digitaalisesti esimerkiksi suljetun verkon päätelaitteen ja tunnuksen avulla. Tunnus voi olla esimerkiksi edellä mainitun tapainen tunnusluku. Tunnuksen antamisen jälkeen sanoma voidaan allekirjoittaa ja lähettää suljetun langattoman verkon 206 välityksellä suljetun verkon palveluntuottajalle 205 vaiheessa 3.0. Sanoma voidaan salata esimerkiksi päätelaitteen SIM-korttiin 220 tallennetun salaussalaimen 221 ja päätelaitteessa olevan prosessorin 222 avulla. Palveluntuottaja 205 voi tunnistaa palvelunkäyttäjän 223 suljetun verkon päätelaitteen 207 ja välittää 204 allekirjoitetun sanoman avoimen verkon palveluntuottajalle 203, joka välittää sanoman edelleen palvelunkäyttäjän 223 avoimen verkon päätelaitteelle 301 avoimen verkon 202 välityksellä vaiheessa 3.1.

Palvelunkäyttäjän 223 päätelaite 301 voi olla esimerkiksi sopivilla muistiyksiköillä, tietoliikenneyhteydellä ja prosessorilla varustettu työasema tai tietokone, PDA, matkapuhelin, digiTV tai vastaava järjestelmä, jolla voidaan vastaanottaa edellä mainittu kaltainen verkkolomake sekä lähettää allekirjoituspyyntö ja vastaanottaa allekirjoitettu sanoma. Palvelunkäyttäjän päätelaitteessa 301 on tyypillisesti välineet 302 lomakkeen hakemiseksi, vastaanottamiseksi ja käsittelemiseksi sekä välineet 303 allekirjoituspyynnön lähettämiseksi ja allekirjoituksen vastaanottamiseksi.

Palvelunkäyttäjän 223 suljetussa verkossa toimiva päätelaite 207 on tyypillisesti PDA, matkapuhelin tai vastaavan kaltainen järjestelmä, jolla voidaan hyväksyä vas-

taanotettu allekirjoituspyyntö esimerkiksi näppäilemällä tietty tunnus tai tunnusluku. Erityisesti päätelaite 207 voi olla langattomassa verkossa toimiva matkapuhelin, joka on varustettu sopivalla SIM-kortilla 220, SIM-korttiin tallennetulla salausavaimella 221 sekä lisäksi mahdollisesti myös prosessorilla 222. Prosessori mahdollistaa mm. sähköisen allekirjoituksen käytön sekä matkapuhelimen avulla tehtävän ja salauksen vaatiman laskutoimituksen suorittamisen.

Lisäksi avoimen ja suljetun verkon palveluntuottajien järjestelmissä voi olla keskenään samoja välineitä osapuolten tunnistamiseksi ja tiedon välittämiseksi, jolloin tietojen välittäminen palvelunkäyttäjän 223 avoimen verkon päätelaitteen 301 ja suljetun verkon päätelaitteen 207 välillä voidaan hoitaa joko vaihtoehtoisesti vain avoimen tai vain suljetun verkon palveluntuottajan välityksellä. Tapahtumaan liittyvien osapuolten tunnistaminen palveluntuottajien avulla suoritetaan edullisesti aina välitettäessä tapahtumaan liittyvää tietoa. Tieto voidaan vaihtoehtoisesti välittää myös kolmannen luotettavan osapuolen välityksellä, jolloin tietojen eheys sekä muut vastaavat tietoturvaluusteet, tiedon varmistamiseen ja osapuolten luotettavaan tunnistamiseen liittyvät toimenpiteet voidaan suorittaa mainitun kolmannen luotettavan osapuolen avulla.

Kuva 4 esittää vuokaaviona erästä keksinnön mukaista menetelmää tuotteen tai palvelun maksamiseksi 401. Vaiheessa 402 asiakas ostaa tuotteen ja vaiheessa 403 myyjä siirtää asiakkaan kauppatahtumatiedot kassa- ja laskutusjärjestelmäänsä, joka on yhteydessä esimerkiksi avoimeen tietoverkkoon, kuten Internet-tietoverkkoon. Vaiheessa 404 myyjän laskutusjärjestelmästä välitetään kauppatahtumatiedot tyypillisesti Internet-tietoverkon välityksellä avoimen verkon palveluntuottajan järjestelmään. Palveluntuottaja voi olla esimerkiksi tietoverkon verkko-operaattori, joka tarjoaa tietoverkko- tai Internet-palveluita ja jonka kanssa myyjä on mahdollisesti tehnyt palvelusopimuksen. Avoimen verkon palveluntuottaja voi tässä vaiheessa tunnistaa myyjän ja välittää kauppatahtumatiedot edelleen suljetun verkon palveluntuottajalle vaiheessa 405. Suljetun verkon palveluntuottaja voi olla esimerkiksi langattoman verkon verkko-operaattori, joka puolestaan voi tunnistaa langattomassa verkossa olevan asiakkaan päätelaitteen ja välittää kauppatahtumatiedot edelleen päätelaitteelle vaiheessa 406. Vaihtoehtoisesti myös avoimen verkon palveluntuottaja voi tunnistaa asiakkaan ja välittää tapahtumatiedot suoraan asiakkaan päätelaitteelle vaiheessa 406.

Asiakkaan saadessa kauppatahtumatiedot suljetun verkon päätelaitteelleen hän voi varmistua kauppatahtumatietojen oikeellisuudesta vaiheessa 407. Kauppatahtumatiedot voidaan myös salata esimerkiksi jollain salausalgoritmilla, jolloin vai-

heessa 407 suoritetaan myös salauksen purku ja tapahtumatietojen esittäminen selkokielisesti. Vaiheessa 408 asiakas voi valita, hyväksyykö hän tapahtumatiedot vai ei. Tuotteen tai palvelun maksaminen keskeytetään vaiheessa 409, jos asiakas ei hyväksy tapahtumatietoja. Jos asiakas hyväksyy tiedot, suoritetaan maksaminen vaiheessa 410 antamalla suljetun verkon päätelaitteelle esimerkiksi edellä mainitun kaltainen tunnus.

Vaiheessa 411 asiakkaan antama tunnus todennetaan esimerkiksi vertaamalla annettua tunnusta päätelaitteen SIM-kortin tietoihin. Jos annettu tunnus on oikein, lähetetään tieto maksun suorittamisesta vaiheessa 413 suljetun verkon palveluntuottajalle. Maksutieto voidaan lähettää myös suoraan avoimen verkon palveluntarjoajalle vaiheessa 412. Lähettävä tieto voidaan myös salata ennen lähetystä esimerkiksi suljetun verkon päätelaitteen SIM-kortille tallennetun salausavaimen ja päätelaitteessa mahdollisesti olevan prosessorin avulla.

Suljetun verkon palveluntuottaja voi tunnistaa suljetun verkon päätelaitteen ja päätelaitteen käyttäjän vaiheen 413 yhteydessä ja välittää tiedon edelleen avoimen verkon palveluntuottajan järjestelmään vaiheessa 412. Avoimen verkon palveluntuottaja voi tunnistaa kauppatapahtumaan liittyvän myyjän vaiheen 412 yhteydessä ja välittää tiedon maksusuorituksesta edelleen myyjän laskutusjärjestelmään vaiheessa 414. Vaihtoehtoisesti tietojen välittäminen tapahtuman eri osapuolten välillä voidaan toteuttaa joko yksistään vain suljetun tai vain avoimen verkon palveluntuottajan avulla, jolloin molemmat tietojen välittäjät (palveluntuottajat) voivat tunnistaa molemmat tapahtuman osapuolet.

Kuva 5 esittää vuokaaviona erästä keksinnön mukaista menetelmää lomakkeen digitaaliseksi allekirjoittamiseksi 501. Vaiheessa 502 sähköistä verkkolomaketta voidaan tarjota esimerkiksi tietoverkossa, josta se voidaan vaiheessa 503 noutaa palvelunkäyttäjän avoimen verkon päätelaitteelle, kuten esimerkiksi tietokoneelle tai muulle vastaavalle laitteelle, jatkotoimenpiteitä varten. Lomake voidaan toimittaa myös muilla tavoin tai se voidaan vaihtoehtoisesti luoda myös palvelunkäyttäjän avoimen verkon päätelaitteella. Jos lomake on toimitettu palveluntuottajan järjestelmästä palvelunkäyttäjän avoimen verkon päätelaitteelle esimerkiksi tietoverkon välityksellä, voidaan vaiheessa 504 lähettää palveluntuottajalle kuittaus lomakkeen vastaanottamisesta ja vastaanottamisen onnistumisesta.

Lisäksi vaiheiden 502 ja 503 aikana voidaan suorittaa osapuolten tunnistaminen, jos haettava verkkolomake sitä vaatii. Tällainen verkkolomake voi olla esimerkiksi verotoimistosta tai vastaavasta paikasta lähetettävä ko. palvelunkäyttäjän tiedoilla varus-

tettu lomake, joka toimitetaan tietoturvasyistä johtuen vain asianomaiselle palvelunkäyttäjälle. Tällöin palvelunkäyttäjälle voidaan lähettää tämän päätelaitteelle allekirjoitus- tai varmennuspyyntö tässä selostuksessa esitettyjen suoritustapojen mukaisesti, jolloin voidaan varmistua palvelunkäyttäjän identiteetistä ja oikeuksista mainitun lomakkeen noutamiseen tietoverkon avulla.

Palvelunkäyttäjä voi tehdä saamalleen lomakkeelle erilaisia toimenpiteitä, kuten esimerkiksi muokata, lähettää, arkistoida tai allekirjoittaa sen. Vaiheessa 505 voidaan päättää, allekirjoitetaanko lomake vai ei. Vaiheessa 506 suoritustapojen mukainen menetelmä lopetetaan, jos lomake päätetään olla allekirjoittamatta. Jos lomake puolestaan päätetään allekirjoittaa, voidaan avoimen verkon palveluntuottajalle lähettää allekirjoituspyyntö vaiheessa 507. Vaiheessa 507 avoimen verkon palveluntuottaja voi myös tunnistaa allekirjoitustapahtumaan liittyvät osapuolet. Allekirjoituspyyntö voidaan lähettää palvelunkäyttäjän avoimen verkon päätelaitteella tai vaihtoehtoisesti myös palvelunkäyttäjän suljetun verkon päätelaitteella. Avoimen verkon palveluntuottaja voi välittää allekirjoituspyynnön edelleen suljetun verkon palveluntuottajalle vaiheessa 508, jolloin suljetun verkon palveluntuottaja voi tunnistaa palvelunkäyttäjän suljetun verkon päätelaitteen ja jatkolähetää pyynnön edelleen päätelaitteelle vaiheessa 509. Vaihtoehtoisesti myös avoimen verkon palveluntuottaja voi tunnistaa palvelunkäyttäjän suljetun verkon päätelaitteen ja jatkolähetää allekirjoituspyynnön suoraan palvelunkäyttäjän suljetun verkon päätelaitteelle vaiheessa 509.

Saatuana allekirjoituspyynnön suljetun verkon päätelaitteelleen palvelunkäyttäjä voi allekirjoittaa pyynnön antamalla tunnuksen päätelaitteelle vaiheessa 510. Tunnus voi olla esimerkiksi edellä mainitun tyyppinen tunnusluku. Vaiheessa 511 käyttäjän antama tunnus todennetaan. Allekirjoitus voidaan haluttaessa myös salata tunnuksen antamisen jälkeen esimerkiksi päätelaitteen SIM-kortille tallennetun salausavaimen ja päätelaitteessa mahdollisesti olevan prosessorin avulla. Allekirjoitus voidaan lähettää suljetun verkon palveluntuottajalle 205 vaiheessa 513, jolloin palveluntuottaja voi tunnistaa palvelunkäyttäjän suljetun verkon päätelaitteen ja välittää allekirjoituksen edelleen avoimen verkon palveluntuottajalle 203 vaiheessa 512. Allekirjoitus voidaan lähettää käyttäjän suljetun verkon päätelaitteelta 207 vaihtoehtoisesti myös suoraan avoimen verkon palveluntuottajalle 203 vaiheessa 512, jolloin avoimen verkon palveluntuottaja voi tunnistaa käyttäjän suljetun verkon päätelaitteen 207. Avoimen verkon palveluntuottaja voi tunnistaa tyyppillisesti myös palvelunkäyttäjän avoimen verkon päätelaitteen 301 ja välittää allekirjoituksen edelleen päätelaitteelle 301 vaiheessa 514.

Edellä on esitetty vain eräitä keksinnön mukaisen ratkaisun suoritusmuotoja. Keksinnön mukaista periaatetta voidaan luonnollisesti muunnella patenttivaatimusten määrittelemän suoja-alueen puitteissa esimerkiksi toteutuksen yksityiskohtien sekä käyttöalueiden osalta. Erityisesti käytettävät päätelaitteet voivat olla minkä tahansa 5 tyyppisiä järjestelmiä, joiden avulla keksinnön mukaista ideaa voidaan käyttää tai soveltaa. Lisäksi avoimen ja suljetun verkon palveluntuottajien menetelmät ja järjestelmät voivat olla joissain tapauksissa samoja, jolloin esimerkiksi lomakkeen haku tai allekirjoituspyyntö voidaan suorittaa tai välittää vaihtoehtoisesti kumman palveluntuottajan avulla tahansa.

Patenttivaatimukset

1. Menetelmä (101) palvelun tarjoamiseksi tietoverkossa, **tunnettu** siitä, että siirretään (102) avoimessa verkossa palvelutapahtumaan liittyvää tietoa, hyväksytään (104) mainittu tieto ja suoritetaan tiedon hyväksyjän tunnistaminen (107) suljetussa verkossa suoritettavan todentamisen avulla.
- 2 Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainittu tiedon hyväksyminen käsittää vaiheet, joissa
 - suoritetaan (104) mainittuun palvelutapahtumaan liittyvän tiedon hyväksymisen syöttämällä suljetun verkon päätelaitteelle (207) tunnus,
- 10 - tunnistetaan ja todennetaan (105) mainittu päätelaitteelle syötetty tunnus, ja
 - siirretään (412, 413) mainittu palvelutapahtuman hyväksymiseen liittyvä tieto palveluntuottajalle (203, 205) suljetun verkon avulla.
3. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainittu palvelutapahtuma on kauppapahtuma (401).
- 15 4. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainittu palvelutapahtuma on lomakkeen digitaalinen allekirjoittaminen (501).
5. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että tiedon siirtämiseen liittyvät osapuolet tunnistetaan palveluntuottajan (203, 205) avulla.
6. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että tiedon siirtämiseen liittyvät osapuolet tunnistetaan kolmannen luotettavan osapuolen avulla.
- 20 7. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainittu päätelaitteella (207) annettava tunnus on SIM-kortilla (220) todennettavissa oleva PIN-luku.
8. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainittuun palvelutapahtumaan liittyvän tiedon salauksen purkaminen suoritetaan palvelunkäyttäjän päätelaitteen (207) avulla.
- 25 9. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainitun palvelutapahtuman hyväksymiseen liittyvä tieto salataan palvelunkäyttäjän päätelaitteen avulla (207).

10. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainitut palvelutapahtumatiedot lähetetään palvelunkäyttäjän järjestelmästä (201, 301) palveluntuottajan (203, 205) järjestelmään avoimen tietoverkon (202) välityksellä.

5 11. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainitun palvelutapahtuman hyväksymiseen liittyvä tieto lähetetään palveluntuottajan (203, 205) järjestelmään suljetun verkon (206) välityksellä.

12. Järjestelmä (200, 300) palvelun tarjoamiseksi tietoverkossa, **tunnettu** siitä, että järjestelmä käsittää avoimen (202) ja suljetun (206) tietoverkon, välineet (208, 303) palvelutapahtumaan liittyvän tiedon siirtämiseksi avoimessa verkossa, välineet (213) mainitun tiedon hyväksymiseksi ja välineet (216) tiedon hyväksyjän tunnistamiseksi
10 suljetussa verkossa suoritettavan todentamisen avulla.

13 Patenttivaatimuksen 12 mukainen järjestelmä, **tunnettu** siitä, että mainittu tiedon hyväksyminen käsittää lisäksi

- välineet (213) mainittuun palvelutapahtumaan liittyvän tiedon hyväksymiseksi
15 syöttämällä suljetun verkon päätelaitteelle (207) tunnus,

- välineet (214) mainitun päätelaitteelle syötetyn tunnuksen tunnistamiseksi ja todentamiseksi, ja

- välineet (215) mainitun palvelutapahtuman hyväksymiseen liittyvän tiedon siirtämiseksi palveluntuottajalle (203, 205) suljetun verkon (206) avulla.

20 14. Patenttivaatimuksen 12 mukainen järjestelmä, **tunnettu** siitä, että mainittu suljettu verkko (206) on matkapuhelinverkko.

15. Patenttivaatimuksen 12 mukainen järjestelmä, **tunnettu** siitä, että mainittu avoin verkko (202) on Internet-tietoverkko.

25 16. Patenttivaatimuksen 13 mukainen järjestelmä, **tunnettu** siitä, että mainittu suljetun verkon päätelaite (207) on langaton päätelaite.

17. Patenttivaatimuksen 16 mukainen järjestelmä, **tunnettu** siitä, että mainitussa päätelaitteessa (207) on SIM-kortti (220).

18. Patenttivaatimuksen 16 mukainen järjestelmä, **tunnettu** siitä, että mainitun päätelaitteen (207) SIM-kortissa (220) on tallennettuna salausavain (221).

19. Patenttivaatimuksen 16 mukainen järjestelmä, tunnettu siitä, että mainitussa päätelaitteessa (207) on prosessori (222) tiedon salaamiseksi ja salauksen purkamiseksi.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

(57) Tiivistelmä

Keksinnön kohteena on menetelmä ja järjestelmä (300) palvelun tarjoamiseksi avointa (202) ja suljettua (206) verkkoa käyttäen. Erityisesti keksintö koskee palvelutapahtumaan liittyvien tunnistetietojen välittämistä eri osapuolten ja -järjestelmien välillä. Keksinnön eräänä ajatuksena on se, että palvelutapahtumaan liittyvää tietoa siirretään palvelunkäyttäjän 223 suljetun verkon päätelaitteelle (207) palvelun hyväksymistä tai palvelunkäyttäjän identifioimista varten. Palvelun hyväksyminen tai käyttäjän tunnistaminen on mahdollista suorittaa antamalla palvelunkäyttäjän päätelaitteella (207) tunnus. Lisäksi keksinnön eräänä ajatuksena on palvelutapahtuman osapuolten (223, 224) luotettava tunnistaminen ja todentaminen palveluntuottajan (203, 205) tai kolmannen luotettavan osapuolen avulla.

Fig. 2